How to Perform an Operational Risk Assessment Guidelines

Office of Risk Management

Carleton University

The guidelines that follow should be used to implement a Departmental or Project specific risk assessment. It is the responsibility of the Department Head or Project Manager to determine the life cycle of the Risk Management Process for the Department or Project. (*For example, the Manager of a Department may wish to go through the process monthly or semi-annually, while a project manager may see the need to do it bi-weekly*).

1. **Identify Departments Goals -** The first step is to identify the unit's or project's principal goals and objectives, and the critical success factors to achieve them. What are the key things that must be done in order to accomplish objectives? Objectives include operational objectives (e.g., pay all employees the correct amount on time) as well as compliance objectives, such as compliance with laws and regulations (e.g., Occupational Health and Safety legislation). The following questions will he;lp to identify the department's goals and risks of the project.

   Risk Assessment Questionnaire

   - What is the Mission/Purpose of the unit? What are its principal goals and objectives?
   - What is of most concern to you regarding the attainment of the unit's goals and objectives?
   - For each of the unit's principal goals and objectives, identify events or circumstances that may interfere with or prevent its achievement.
   - Have there been changes in external factors such as laws and regulations?
   - Have the terms of contracts changed? Are contracts up for renewal? If a contract is not renewed, is a contingency plan required, and if so, is there one?
   - Have there been changes in key personnel during the past year?
   - Has there been high staff turnover in the past few years?
   - Has the staff received appropriate training?
   - Are the unit's business processes simple and routine or complex and non-routine?
   - Are procedures and processes documented, i.e., procedure manuals?
   - Have other units in other organizations failed to accomplish similar objectives? Why?
   - Have there been changes in information systems in the past year?
   - Has the unit taken on new activities? Has there been internal restructuring?
   - What risks have increased or decreased during the past year? Why?
   - Does the unit have a contingency plan if there were a major disruption in provision of services, e.g., all staff on leave of absence, information systems crash, and permanent loss of facilities or key personnel, all paper records destroyed?

2. Risk Identification - Second, identify the risks that are the potential causes of failing to achieve the goals and objectives. Examples of risks are: loss of program accreditation, non-performance of research contracts, destruction of important paper or electronic files without backup, sudden loss or destruction of physical assets, occurrence of events, contracts or damages in excess of amounts insured, loss of an important source of income, large over-expenditures, invalid data on file and an information systems crash. Significant risks should be identified even if insured.

Identified risks to your department go in the Column 1 of the Operational Risk Assessment Worksheet. (Appendix A).

Column 2 of the Risk Assessment Worksheet asks for risk factors. Risks arise from external and internal factors. External factors can include but not limited to: government funding; changing student and customer needs and expectations; competition; new legislation and regulations; technological developments; and economic changes. Internal factors include disruption in computer processing; employee competence, training and motivation; and change in key personnel. A knowledge of risk factors assists in identifying important risks.

3. Risk Analysis - The third step involves risk analysis, which is estimating the significance of a risk in terms of the *Impact* (Column 3 to 8) on the department, project or the university and assessing the *Likelihood* of the risk occurring (Column 9). In practice, one estimates the significance of a risk when it is identified in order to discard insignificant risks immediately; otherwise the list of risks could be infinite. Potential losses should be quantified in financial terms whenever possible. The likelihood or probability of a significant risk occurring is also assessed. A risk that does not have a significant impact on the department, project or university and has a very low likelihood of occurrence does not warrant serious concern. Very high risks with a high likelihood of occurrence do warrant concern.

Use Table 1 Risk Impact Rating as a guide to assess the score for every identified risk against each of the Impact Rating Categories. The *Likelihood* score is determined using Table 2 Risk Likelihood Ratings.

4. Risk Evaluation - Risk Scores are calculated by taking the score for the highest *Impact* category of each risk and multiplying it by the score for *Likelihood*. The scores for each risk provide a Risk Ranking which enables each risk on the Risk Register to be ranked and then categorized into one of the following three categories:

Green – (Score 0-10)	Risk Acceptable – No additional mitigation required
Yellow – (Score 11-15)	Risk Acceptable – Additional mitigation may be required in the future
Red – (Score 16-25)	High Risk – Ongoing monitoring and additional mitigation required

All risks identified as significant risks that are beyond the ability or authority of the Department or Project to mitigate must be reported to the appropriate Director and/or Vice-President.

5. Risk Treatment - The next step in risk assessment is consideration of how the risk should be managed. What actions are being taken or need to be taken to reduce the significance and/or likelihood of the risk occurring? What are the costs involved? What level of risk is acceptable to management? Actions taken or that need to be taken are reported in the Column 11 “Action Taken”. The manager or academic leader should assign to staff or project personnel responsibility for carrying out the actions needed to mitigate the risk and have them report the results of the actions taken.

6. Reassessment - The final step is to reassess risk at appropriate intervals by following steps one through five.

7. Reporting - A copy of the completed Operational Risk Assessment must be submitted to the office of Risk Management so it can be used as an input into the Enterprise Risk Management process (if necessary).

For additional information on how to complete a department or project risk assessment contact the Risk and Insurance Manager at risk@carleton.ca.

Example - Operational Risk Assessment Example for Capital Construction Project

The university decides to build a new addition to the Mackenzie Building and an operational risk assessment is required as per the Enterprise Risk Management Framework.

Step 1 – First step of the operational risk management process is to determine the projects goals. The goal for the project is to have the extension completed on time and on budget and when completed to provide more student space.

Step 2 – The second step is to identify the risks which could prevent the project from being completed on time, on budget and have the new space meet the needs of students. To identify risks, conduct a brain storming session with the project team to identify all possible risks to the project in column 1 list all risks identified and in column 2 list some of the risks factors which contribute to the risk. (See example below).

Step 3 – The third step is risk analysis. Using the Likelihood Chart in Table 2 establish the Likelihood of the risk occurring (for the risks identified). In the example below, the first risk identified is the land where the new extension is to be built is contaminated. The likelihood for this risk to occur is determined to be possible, as the land was previously used as a dump. Then using the Impact Chart in Table 1 rate the impact of the six impact categories listed. On the example risk register below each impact category has been rated using the chart with highest rated impact was on the Operational category.

Step 4 – The fourth step is evaluating the risk. This step involves ranking the risks identified using the likelihood score and the impact score to obtain the risk score. For the contamination risk in the example, the likelihood rating is 3 or Possible and the highest Impact ratings are in the Operation and Legal categories with a score of 4 or serious. Multiply the Likelihood score (3) by the highest risk impact score (4) to obtain a risk score (12) for each risk. Rank the risks using the risk score from the highest to lowest. Indicate the trend of the risk, is it increasing or decreasing from the previous reporting period. In the example risk register below no trend is indicated as this is an initial risk assessment.

Step 5 – The fifth step is to develop a risk treatment plan to reduce the frequency and/or impact of the identified risks. In the example below the highest ranked risks are site contamination and steel costs. The risk treatment for the contaminated land risk was to ensure that the drilling of test holes will follow industry standards. For the steel price risk, the risk mitigation plan is to arrange for a fixed price contract with the steel supplier. Each risk treatment should be documented in the last column of the risk registry.

Operational Risk Assessment Example Results for Capital Construction Project

Risk	Risk Factor	Strategic	Legal	Operational	Technological	Financial	Reputational	Likelihood	Risk Score	Action Taken
Contaminated project site	Contaminates were dumped on site 50 years ago.Geo-technical consultant did not drill sufficient test holes to identify contaminants	1	4	4	1	1	3	3	12	Approach to soil sampling will follow industry standards
Steel costs rise above budgeted costs	Trade tariffs placed on steel from outside Canada. Strike at steel provider.	1	1	4	1	4	2	3	12	Enter into fix cost contract with supplier. Changing design to reduce amount of steel used in building
Possible delay is obtaining exterior brick	Kiln which produces brick damaged by fire strike at supplier.	1	2	4	1	4	2	2	8	Contingency plan is to order different brick to match

Appendix A - Operational Risk Assessment Worksheet

Department/Project: _____

Prepared by: _____

Risk	Risk Factor	Strategic	Legal	Operational	Technological	Financial	Reputational	Likelihood	Risk Score	Action Taken

Table 1: Risk Impact Rating

Score	Impact of Risk	Strategic	Legal	Operational	Technological	Financial	Reputational
5	Very Serious	Activity does not support any pillar in Strategic Plan or other Strategic planning documents or policies	Potential for major litigation Termination of Contracts for Default Criminal charges for on compliance of regulation	Activity has potential for internal/external fraud, injury to students or workers, damage to physical assets, business disruption, changes to processes	Requirement for major change to Enterprise IT system or significant upgrade to several Faculty/Department significant IT systems. Create single point of failure to critical system(s). Requires collection of large amount of personal data (i.e. whole community)	Financial exposure of activity is $4,000,000 and up	Growing Significant coverage in National, International and Social Media
4	Serious	Activity supports one of the Pillars in the Strategic Plan and one other planning document or policy	Potential for single major or numerous moderate litigations. Potential for increase for default of contract or increased assumption of risk assumed under contract. Potential for fines and orders under regulation	Activity has potential for injury to students or workers, damage to physical assets, business disruption, changes to processes	Requirement for significant change to Enterprise IT system or several Faculty/Department IT systems. Requires collection of significant amount of personal data (i.e. all students or large research sample)	Financial exposure of activity is between $3,000,000 and $4,000,000	Wide Coverage in National and Social Media
3	Moderate	Activity supports two of the Pillars in the Strategic Plan and two other planning documents or policies	Single moderate litigation or numerous small litigations. Contract terms provide some form of indemnity for the university but not completely reciprocal. Potential rescinding of licenses required by regulation	Activity has potential for damage to physical assets, business disruption, changes to processes	Requirement for changes to several Faculty/Department IT systems. Requires collection of data from several group of 2000 or less	Financial exposure of activity between $2,000,000 and $3,000,000	Some coverage in Regional Media (but controlled) and low level of coverage in social media
2	Minor	Activity supports three of the Pillars in the Strategic Plan and two other planning documents or policies	Single minor litigation Reciprocal indemnity included in contract Minimum compliance with regulation	Activity has potential for damage to physical assets, changes to processes	Requirement for changes to one Faculty/Department IT system Requires collection of data from one group of 1000 or less	Financial exposure of activity is between $1,000,000 and $2,000,000	Minor coverage in local and social media
1	Low	Activity supports all four of the Pillars in the Strategic Plan and two other planning documents or policies	Threat of litigation required small payout Indemnity clause fully in favour of the university. Risk fully transferred university exceeds requirement for compliance under regulation	Activity has potential for changes to processes	No IT system changes required No collection of personal data	Financial exposure of activity is between 0 and $1,000,000	No mention in any news or social media

Table 2 Risk Likelihood Rating

Frequency	Risk Probability
Almost Certain - 5	*81-100%* Quite Probable the risk will occur
Likely - 4	*61-80%* More Likely than not this risk will occur in the next 36 months
Possible - 3	*41-60%* Somewhat Likely this loss will occur in the next 36 months
Unlikely - 2	*21-40%* Low possibility this risk will occur in the next 36 months
No Chance or Rare - 1	*1-20%* Very low possibility this risks will occur in the next 36 months